PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-264685
(43)Date of publication of application : 19.09.2003

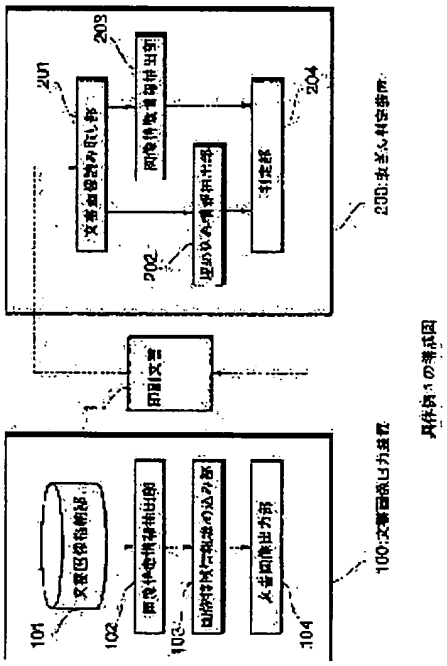
(51)Int.Cl. H04N 1/387
B41J 5/30
B41J 29/38
G06T 1/00
G09C 1/00
G09C 5/00

(21)Application number : 2002-062934
(22)Date of filing : 08.03.2002

(71)Applicant : OKI ELECTRIC IND CO LTD
(72)Inventor : SUZAKI MASAHIKO

(54) DOCUMENT IMAGE OUTPUT METHOD AND APPARATUS, TAMPERING JUDGING METHOD AND SYSTEM, AND PROGRAM FOR CONTROLLING TAMPERING JUDGING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To easily detect a tampering even when printed matter is tampered.
SOLUTION: An image feature information extracting part 102 extracts image feature information from a document image. An image feature information embedding part 103 integrally applies the image feature information to a document as the original image feature information of the document, and a document image output part 104 outputs the documents as a print document 1. When the print document 1 is applied to a tampering judging apparatus 200 as a target document to be judged, that document image is read by a document image reading part 201. An image feature information extracting part 203 extracts the image feature information of the target document to be judged. An embedded information extracting part 202 extracts the original image feature information out of the image of the target document to be judged. A judgment part 204 compares the original image feature information and the image feature information of the target document to be judged and when a difference degree is beyond a prescribed range, the presence of the tempering in the target document to be judged is judged.



LEGAL STATUS

[Date of request for examination] 31.01.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 3804012
[Date of registration] 19.05.2006
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－264685
（Ｐ２００３－２６４６８５Ａ）
(43)公開日　平成15年９月19日(2003.9.19)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
H04N 1/387		H04N 1/387		2C061
B41J 5/30		B41J 5/30	Z	2C187
29/38		29/38	Z	5B057
G06T 1/00	500	G06T 1/00	500 B	5C076
G09C 1/00	640	G09C 1/00	640 D	5J104

審査請求　有　請求項の数16　ＯＬ　（全13頁）　最終頁に続く

(21)出願番号　特願2002－62934(Ｐ2002－62934)

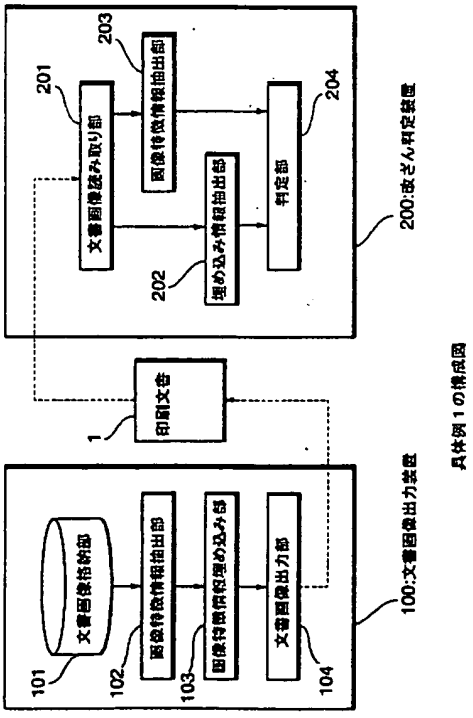
(22)出願日　平成14年３月８日(2002.3.8)

(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号
(72)発明者　須崎　昌彦
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内
(74)代理人　100082050
弁理士　佐藤　幸男

最終頁に続く

(54)【発明の名称】文書画像出力方法及び装置、改ざん判定方法及びシステム、並びに改ざん判定システムの制御用プログラム

(57)【要約】
【課題】　印刷物に対して改ざんが行われた場合でもこれを容易に検出する。
【解決手段】　画像特徴情報抽出部１０２は文書画像から画像特徴情報を抽出する。画像特徴情報埋め込み部１０３は、画像特徴情報を文書の元画像特徴情報として文書に一体に付与し、文書画像出力部１０４はこれを印刷文書１として出力する。改ざん判定装置２００に判定対象文書として印刷文書１が与えられた場合、その文書画像を文書画像読み取り部２０１で読み取る。画像特徴情報抽出部２０３は、判定対象文書の画像特徴情報を抽出する。埋め込み情報抽出部２０２は、判定対象文書の画像中から元画像特徴情報を抽出する。判定部２０４は、これら元画像特徴情報と判定対象文書の画像特徴情報とを比較し、相違度が所定の範囲以上であれば、判定対象文書に対して改ざんがあったと判定する。



具体例１の構成図

1

【特許請求の範囲】

【請求項１】　文書の画像特徴情報をデータ化し、当該データを前記文書の元画像特徴情報として、前記文書と一体に付与して出力する文書画像出力方法。

【請求項２】　請求項１に記載の文書画像出力方法において、

文書画像を複数のブロックに分割し、各ブロック毎に画像特徴情報を求め、これら画像特徴情報を元画像特徴情報とすることを特徴とする文書画像出力方法。

【請求項３】　請求項１または２に記載の文書画像出力方法において、

元画像特徴情報を光学的に読み取り可能なデータとして文書上に印刷することを特徴とする文書画像出力方法。

【請求項４】　文書の画像特徴情報をデータ化し、当該データを暗号鍵として任意の隠し情報を暗号化し、当該暗号化情報を前記文書と一体に付与して出力する文書画像出力方法。

【請求項５】　文書の画像特徴情報をデータ化する画像特徴情報抽出部と、

前記画像特徴情報抽出部が抽出したデータを前記文書の元画像特徴情報として文書に付与する画像特徴情報埋め込み部と、

前記元画像特徴情報が付与された文書を出力する文書画像出力部とを備えたことを特徴とする文書画像出力装置。

【請求項６】　請求項５に記載の文書画像出力装置において、

文書画像を複数のブロックに分割し、各ブロック毎に画像特徴情報を求める画像特徴情報抽出部を備えたことを特徴とする文書画像出力装置。

【請求項７】　請求項５または６に記載の文書画像出力装置において、

元画像特徴情報を光学的に読み取り可能なデータとして文書に付与する画像特徴情報埋め込み部と、

前記元画像特徴情報が付与された文書を印刷出力する文書画像出力部とを備えたことを特徴とする文書画像出力装置。

【請求項８】　文書の画像特徴情報をデータ化する画像特徴情報抽出部と、

前記画像特徴情報抽出部が抽出したデータから暗号鍵を生成する暗号鍵生成部と、

前記暗号鍵生成部で生成した暗号鍵を用いて任意の隠し情報を暗号化する隠し情報暗号化部と、

前記暗号化された隠し情報を前記文書に付与する暗号ブロック埋め込み部と、

前記暗号化された隠し情報が付与された文書を出力する文書画像出力部とを備えたことを特徴とする文書画像出力装置。

【請求項９】　文書の画像特徴情報をデータ化し、当該データを前記文書の元画像特徴情報として、前記文書と

2

一体に付与して出力し、

元画像特徴情報が一体に付与された判定対象文書に対して、前記元画像特徴情報を抽出し、当該元画像特徴情報と、前記判定対象文書の画像から生成した画像特徴情報とを比較して前記判定対象文書に対する改ざんの有無を判定する改ざん判定方法。

【請求項１０】　請求項９に記載の改ざん判定方法において、

文書画像を複数のブロックに分割し、各ブロック毎に画像特徴情報を求め、これら画像特徴情報を元画像特徴情報とすることを特徴とする改ざん判定方法。

【請求項１１】　文書の画像特徴情報をデータ化し、当該データを暗号鍵として任意の隠し情報を暗号化し、当該暗号化情報を前記文書と一体に付与して出力し、

暗号化情報が一体に付与された判定対象文書に対して、当該判定対象文書の画像から画像特徴情報を生成すると共に、当該生成した画像特徴情報から暗号鍵を生成し、当該暗号鍵を用いて前記暗号化情報を復号し、その結果に基づいて前記判定対象文書に対する改ざんの有無を判定する改ざん判定方法。

【請求項１２】　文書画像出力装置と改ざん判定装置とからなる改ざん判定システムであって、

前記文書画像出力装置は、

文書の画像特徴情報をデータ化する画像特徴情報抽出部と、

前記画像特徴情報抽出部が抽出したデータを前記文書の元画像特徴情報として文書に付与する画像特徴情報埋め込み部と、

前記元画像特徴情報が付与された文書を出力する文書画像出力部とを備え、

前記改ざん判定装置は、

元画像特徴情報が一体に付与された判定対象文書に対して、前記元画像特徴情報を抽出する埋め込み情報抽出部と、

前記判定対象文書の画像から当該判定対象文書の画像特徴情報を抽出する画像特徴情報抽出部と、

前記埋め込み情報抽出部が抽出した元画像特徴情報と、前記画像特徴情報抽出部が抽出した画像特徴情報とを比較して前記判定対象文書に対する改ざんの有無を判定する判定部とを備えたことを特徴とする改ざん判定システム。

【請求項１３】　請求項１２に記載の改ざん判定システムにおいて、

文書画像を複数のブロックに分割し、各ブロック毎に画像特徴情報を求める画像特徴情報抽出部を備えたことを特徴とする改ざん判定システム。

【請求項１４】　文書画像出力装置と改ざん判定装置とからなる改ざん判定システムであって、

前記文書画像出力装置は、

文書の画像特徴情報をデータ化する画像特徴情報抽出部

と、
前記画像特徴情報抽出部が抽出したデータから暗号鍵を生成する暗号鍵生成部と、
前記暗号鍵生成部で生成した暗号鍵を用いて任意の隠し情報を暗号化する隠し情報暗号化部と、
前記暗号化された隠し情報を前記文書に付与する暗号ブロック埋め込み部と、
前記暗号化された隠し情報が付与された文書を出力する文書画像出力部とを備え、
前記改ざん判定装置は、
暗号化情報が一体に付与された判定対象文書に対して、
当該判定対象文書の画像から画像特徴情報を生成する画像特徴情報抽出部と、
前記画像特徴情報から暗号鍵を生成する暗号鍵生成部と、
前記判定対象文書から暗号化情報を抽出する暗号化情報抽出部と、
前記暗号鍵生成部で生成した暗号鍵を用いて前記暗号化情報抽出部で抽出した暗号化情報を復号し、その結果に基づいて前記判定対象文書に対する改ざんの有無を判定する隠し情報復号部とを備えたことを特徴とする改ざん判定システム。

【請求項１５】　文書画像出力装置と改ざん判定装置とからなる改ざん判定システムの制御用プログラムであって、
前記文書画像出力装置を構成するコンピュータを、
文書の画像特徴情報をデータ化する画像特徴情報抽出部と、
前記画像特徴情報抽出部が抽出したデータを前記文書の元画像特徴情報として文書に付与し、一体の文書画像データとして出力する画像特徴情報埋め込み部として機能させ、
かつ、
前記改ざん判定装置を構成するコンピュータを、
前記元画像特徴情報が付与された文書を出力する文書画像出力部と、
元画像特徴情報が一体に付与された判定対象文書に対して、前記元画像特徴情報を抽出する埋め込み情報抽出部と、
前記判定対象文書の画像から当該判定対象文書の画像特徴情報を抽出する画像特徴情報抽出部と、
前記埋め込み情報抽出部が抽出した元画像特徴情報と、
前記画像特徴情報抽出部が抽出した画像特徴情報とを比較して前記判定対象文書に対する改ざんの有無を判定する判定部として機能させるための改ざん判定システムの制御用プログラム。

【請求項１６】　文書画像出力装置と改ざん判定装置とからなる改ざん判定システムの制御用プログラムであって、
前記文書画像出力装置を構成するコンピュータを、

文書の画像特徴情報をデータ化する画像特徴情報抽出部と、
前記画像特徴情報抽出部が抽出したデータから暗号鍵を生成する暗号鍵生成部と、
前記暗号鍵生成部で生成した暗号鍵を用いて任意の隠し情報を暗号化する隠し情報暗号化部と、
前記暗号化された隠し情報を前記文書に付与し、一体の文書画像データとして出力する暗号ブロック埋め込み部として機能させ、
かつ、
前記改ざん判定装置を構成するコンピュータを、
前記暗号化された隠し情報が付与された文書を出力する文書画像出力部と、
暗号化情報が一体に付与された判定対象文書に対して、
当該判定対象文書の画像から画像特徴情報を生成する画像特徴情報抽出部と、
前記画像特徴情報から暗号鍵を生成する暗号鍵生成部と、
前記判定対象文書から暗号化情報を抽出する暗号化情報抽出部と、
前記暗号鍵生成部で生成した暗号鍵を用いて前記暗号化情報抽出部で抽出した暗号化情報を復号し、その結果に基づいて前記判定対象文書に対する改ざんの有無を判定する隠し情報復号部として機能させるための改ざん判定システムの制御用プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、文書が改ざんされているか否かを判定するための文書画像出力方法及び装置、改ざん判定方法及びシステムに関するものである。

【０００２】

【従来の技術】従来、公開情報画像が印刷される印刷媒体に機密情報を記録するための手法として、例えば次のようなものがあった。

［１］特開平９－１５４００７号「機密情報記録方法」
この文献に開示されている技術は、記録使用とする機密情報を二値化し、ドット化されたドット化公開情報データ中に二値化機密情報データを所定の暗号キー情報に従って画素単位で埋め込んで印刷データを作成するようにしたものである。

【０００３】［２］特開平９－１７９４９４号「機密情報記録方法」
この文献に開示されている技術は、記録使用とする機密情報を二値化してブロック化し、その各ブロックの内容を十進数化することにより機密情報ブロックＢ１，Ｂ２，Ｂ３，Ｂ４を作成する。一方、公開情報画像を二値化してこれに基準点マークＲ１～Ｒ４を示すコードＤＲ１を埋め込んだ基準情報データＤＳ１を用意する。そして、一つまたは複数の機密情報ブロックと基準点マークとを対応させ、機密情報ブロックの内容に従う１次元ま

たは２次元距離だけその対応する基準点マークから離れた位置に所定の、または機密情報ブロックの内容に従う位置判別マークＤ１～Ｄ４が印刷されるよう位置判別マークのコードを基準情報データＤＳ１に埋め込み、印刷データを作成するようにしたものである。

【０００４】

【発明が解決しようとする課題】ところで、印刷された内容が住民票や印鑑証明書、領収書などであって、印刷媒体が普通紙であるような場合、例えば、氏名や住所、金額、日付等の文字領域を修正液等で消去して印刷物と同じフォントの文字で上書きしたり、あるいは手書きされた金額等に文字を書き加えて、正式な書類として提出するような不正行為が考えられる。しかしながら、上記従来の技術では、印刷物上に機密情報を埋め込むことが目的であって、公開情報そのものに対する保護はできなかった。即ち、印刷物に対して改ざんを行った場合には、このような改ざんの検出は困難であった。また、印刷物に埋め込む情報と公開情報の内容を一致させた場合、もしくは埋め込む情報と公開情報の内容を関連付けるなどした場合には内容の改ざんチェックを行うことはできる。しかしながら、このようなチェックを自動的に行うには公開情報の内容を機械が認識する機構（例えばＯＣＲ等）を改ざんチェック側で必要とし、システムとして大規模になってしまうという問題点を有していた。

【０００５】

【課題を解決するための手段】本発明は、前述の課題を解決するため次の構成を採用する。

〈構成１〉文書の画像特徴情報をデータ化し、このデータを文書の元画像特徴情報として、文書と一体に付与して出力する文書画像出力方法。

【０００６】〈構成２〉構成１に記載の文書画像出力方法において、文書画像を複数のブロックに分割し、各ブロック毎に画像特徴情報を求め、これら画像特徴情報を元画像特徴情報とすることを特徴とする文書画像出力方法。

【０００７】〈構成３〉構成１または２に記載の文書画像出力方法において、元画像特徴情報を光学的に読み取り可能なデータとして文書上に印刷することを特徴とする文書画像出力方法。

【０００８】〈構成４〉文書の画像特徴情報をデータ化し、このデータを暗号鍵として任意の隠し情報を暗号化し、暗号化情報を文書と一体に付与して出力する文書画像出力方法。

【０００９】〈構成５〉文書の画像特徴情報をデータ化する画像特徴情報抽出部と、画像特徴情報抽出部が抽出したデータを文書の元画像特徴情報として文書に付与する画像特徴情報埋め込み部と、元画像特徴情報が付与された文書を出力する文書画像出力部とを備えたことを特徴とする文書画像出力装置。

【００１０】〈構成６〉構成５に記載の文書画像出力装置において、文書画像を複数のブロックに分割し、各ブロック毎に画像特徴情報を求める画像特徴情報抽出部を備えたことを特徴とする文書画像出力装置。

【００１１】〈構成７〉構成５または６に記載の文書画像出力装置において、元画像特徴情報を光学的に読み取り可能なデータとして文書に付与する画像特徴情報埋め込み部と、元画像特徴情報が付与された文書を印刷出力する文書画像出力部とを備えたことを特徴とする文書画像出力装置。

【００１２】〈構成８〉文書の画像特徴情報をデータ化する画像特徴情報抽出部と、画像特徴情報抽出部が抽出したデータから暗号鍵を生成する暗号鍵生成部と、暗号鍵生成部で生成した暗号鍵を用いて任意の隠し情報を暗号化する隠し情報暗号化部と、暗号化された隠し情報を文書に付与する暗号ブロック埋め込み部と、暗号化された隠し情報が付与された文書を出力する文書画像出力部とを備えたことを特徴とする文書画像出力装置。

【００１３】〈構成９〉文書の画像特徴情報をデータ化し、このデータを文書の元画像特徴情報として、文書と一体に付与して出力し、元画像特徴情報が一体に付与された判定対象文書に対して、元画像特徴情報を抽出し、元画像特徴情報と、判定対象文書の画像から生成した画像特徴情報とを比較して判定対象文書に対する改ざんの有無を判定する改ざん判定方法。

【００１４】〈構成１０〉構成９に記載の改ざん判定方法において、文書画像を複数のブロックに分割し、各ブロック毎に画像特徴情報を求め、これら画像特徴情報を元画像特徴情報とすることを特徴とする改ざん判定方法。

【００１５】〈構成１１〉文書の画像特徴情報をデータ化し、このデータを暗号鍵として任意の隠し情報を暗号化し、暗号化情報を文書と一体に付与して出力し、暗号化情報が一体に付与された判定対象文書に対して、判定対象文書の画像から画像特徴情報を生成すると共に、生成した画像特徴情報から暗号鍵を生成し、暗号鍵を用いて暗号化情報を復号し、その結果に基づいて判定対象文書に対する改ざんの有無を判定する改ざん判定方法。

【００１６】〈構成１２〉文書画像出力装置と改ざん判定装置とからなる改ざん判定システムであって、文書画像出力装置は、文書の画像特徴情報をデータ化する画像特徴情報抽出部と、画像特徴情報抽出部が抽出したデータを文書の元画像特徴情報として文書に付与する画像特徴情報埋め込み部と、元画像特徴情報が付与された文書を出力する文書画像出力部とを備え、改ざん判定装置は、元画像特徴情報が一体に付与された判定対象文書に対して、元画像特徴情報を抽出する埋め込み情報抽出部と、判定対象文書の画像から判定対象文書の画像特徴情報を抽出する画像特徴情報抽出部と、埋め込み情報抽出部が抽出した元画像特徴情報と、画像特徴情報抽出部が抽出した画像特徴情報とを比較して判定対象文書に対す

る改ざんの有無を判定する判定部とを備えたことを特徴とする改ざん判定システム。

【００１７】〈構成１３〉構成１２に記載の改ざん判定システムにおいて、文書画像を複数のブロックに分割し、各ブロック毎に画像特徴情報を求める画像特徴情報抽出部を備えたことを特徴とする改ざん判定システム。

【００１８】〈構成１４〉文書画像出力装置と改ざん判定装置とからなる改ざん判定システムであって、文書画像出力装置は、文書の画像特徴情報をデータ化する画像特徴情報抽出部と、画像特徴情報抽出部が抽出したデータから暗号鍵を生成する暗号鍵生成部と、暗号鍵生成部で生成した暗号鍵を用いて任意の隠し情報を暗号化する隠し情報暗号化部と、暗号化された隠し情報を文書に付与する暗号ブロック埋め込み部と、暗号化された隠し情報が付与された文書を出力する文書画像出力部とを備え、改ざん判定装置は、暗号化情報が一体に付与された判定対象文書に対して、判定対象文書の画像から画像特徴情報を生成する画像特徴情報抽出部と、画像特徴情報から暗号鍵を生成する暗号鍵生成部と、判定対象文書から暗号化情報を抽出する暗号化情報抽出部と、暗号鍵生成部で生成した暗号鍵を用いて暗号化情報抽出部で抽出した暗号化情報を復号し、その結果に基づいて判定対象文書に対する改ざんの有無を判定する隠し情報復号部とを備えたことを特徴とする改ざん判定システム。

【００１９】〈構成１５〉文書画像出力装置と改ざん判定装置とからなる改ざん判定システムの制御用プログラムであって、文書画像出力装置を構成するコンピュータを、文書の画像特徴情報をデータ化する画像特徴情報抽出部と、画像特徴情報抽出部が抽出したデータを文書の元画像特徴情報として文書に付与し、一体の文書画像データとして出力する画像特徴情報埋め込み部として機能させ、かつ、改ざん判定装置を構成するコンピュータを、元画像特徴情報が付与された文書を出力する文書画像出力部と、元画像特徴情報が一体に付与された判定対象文書に対して、元画像特徴情報を抽出する埋め込み情報抽出部と、判定対象文書の画像から判定対象文書の画像特徴情報を抽出する画像特徴情報抽出部と、埋め込み情報抽出部が抽出した元画像特徴情報と、画像特徴情報抽出部が抽出した画像特徴情報とを比較して判定対象文書に対する改ざんの有無を判定する判定部として機能させるための改ざん判定システムの制御用プログラム。

【００２０】〈構成１６〉文書画像出力装置と改ざん判定装置とからなる改ざん判定システムの制御用プログラムであって、文書画像出力装置を構成するコンピュータを、文書の画像特徴情報をデータ化する画像特徴情報抽出部と、画像特徴情報抽出部が抽出したデータから暗号鍵を生成する暗号鍵生成部と、暗号鍵生成部で生成した暗号鍵を用いて任意の隠し情報を暗号化する隠し情報暗号化部と、暗号化された隠し情報を文書に付与し、一体の文書画像データとして出力する暗号ブロック埋め込み部として機能させ、かつ、改ざん判定装置を構成するコンピュータを、暗号化された隠し情報が付与された文書を出力する文書画像出力部と、暗号化情報が一体に付与された判定対象文書に対して、判定対象文書の画像から画像特徴情報を生成する画像特徴情報抽出部と、画像特徴情報から暗号鍵を生成する暗号鍵生成部と、判定対象文書から暗号化情報を抽出する暗号化情報抽出部と、暗号鍵生成部で生成した暗号鍵を用いて暗号化情報抽出部で抽出した暗号化情報を復号し、その結果に基づいて判定対象文書に対する改ざんの有無を判定する隠し情報復号部として機能させるための改ざん判定システムの制御用プログラム。

【００２１】

【発明の実施の形態】以下、本発明の実施の形態を具体例を用いて詳細に説明する。

《具体例１》

〈構成〉図１は、本発明の改ざん判定システムの具体例１を示す構成図である。図示の改ざん判定システムは、文書画像出力装置１００と改ざん判定装置２００からなる。文書画像出力装置１００は、文書の画像特徴情報をデータ化し、このデータを文書の正当な画像情報である元画像特徴情報として文書に付与し、これらを一体に出力する機能を有する装置である。改ざん判定装置２００は、文書画像出力装置１００から出力された印刷文書１のように、判定対象文書中に元画像特徴情報が付与された文書に対して、その判定対象文書の画像特徴情報を抽出し、この画像特徴情報と、元画像特徴情報とを比較することにより、その文書に対する改ざんの有無を判定する機能を有している。これらの装置は、次のように構成されている。

【００２２】文書画像出力装置１００は、文書画像格納部１０１、画像特徴情報抽出部１０２、画像特徴情報埋め込み部１０３、文書画像出力部１０４からなる。文書画像格納部１０１は、文書画像出力装置１００にて印刷出力するための文書画像を格納する機能部であり、磁気記憶装置や半導体メモリといった記憶装置上に実現されている。また、格納されている文書は、印刷イメージ（紙の上に印刷された状態の画像、背景は白画素、文字は黒画素で構成されている）として記憶装置上に展開されているとする。画像特徴情報抽出部１０２は、文書画像の周波数スペクトル等に基づいて画像の特徴情報（元画像特徴情報）を抽出する機能部である。尚、この抽出の詳細については後述する。画像特徴情報埋め込み部１０３は、画像特徴情報抽出部１０２で抽出された元画像特徴情報を数値化し、バーコードのような光学的にデータを読取可能な形式で文書画像の空白部分に挿入し、一体の文書画像データとして出力する機能部である。文書画像出力部１０４は、画像特徴情報埋め込み部１０３で作成した文書画像データを印刷するプリンタであり、印刷文書１は、この文書画像出力部１０４で出力された文

書である。

【００２３】改ざん判定装置２００は、文書画像読み取り部２０１、埋め込み情報抽出部２０２、画像特徴情報抽出部２０３、判定部２０４からなる。文書画像読み取り部２０１は、判定対象文書の画像を光学的に読み取って画像データとして出力するスキャナ等を備えたものであり、読み取った画像に対して回転などの補正や雑音除去といった処理を行う機能や、判定対象文書の画像から元画像特徴情報部分をを切り出すといった機能も有している。埋め込み情報抽出部２０２は、文書画像読み取り部２０１で切り出された元画像特徴情報部分の画像データからバーコードなどの形式で挿入されている元画像特徴情報を復元する機能を有している。画像特徴情報抽出部２０３は、文書画像読み取り部２０１で出力された画像データから元画像特徴情報部分を消去した上で、画像データの画像特徴情報を抽出する機能部であり、これは画像特徴情報抽出部１０２と同様の機能により実現されている。判定部２０４は、埋め込み情報抽出部２０２で抽出された情報（元画像特徴情報）と、画像特徴情報抽出部２０３で新たに抽出した画像特徴情報とを比較して特徴に相違が存在するかを判定し、その判定結果に基づいて印刷文書１に改ざんがあったか否かを判定する機能部である。

【００２４】尚、上記文書画像出力装置１００および改ざん判定装置２００はコンピュータで実現され、文書画像出力装置１００における画像特徴情報抽出部１０２および画像特徴情報埋め込み部１０３と、改ざん判定装置２００における文書画像読み取り部２０１～判定部２０４は、それぞれ対応するソフトウェアと、これらのソフトウェアを実行するためのプロセッサやメモリ等のハードウェアからなるものである。

【００２５】〈動作〉図２は、文書画像出力装置１００の動作を示すフローチャートである。先ず、文書画像格納部１０１に格納されている文書画像が画像特徴情報抽出部１０２に入力される（ステップＳ１０１）。図３は、文書画像の一例を示す説明図である。画像特徴情報抽出部１０２では、文書画像をｎ個の小ブロック画像に分割する（ステップＳ１０２）。図４は、文書画像を分割した状態の説明図である。このように、文書画像を複数のブロック画像に分割するのは印刷文書に対して改ざんが行われた場合に、文書中のどの部分が改ざんされているかを特定できるようにするためであり、多くのブロック画像に分割するほど位置の特定が詳細となる。尚、各ブロック画像の大きさは固定でも良いし、画像中の場所によって変動させてもよいが、ここでは固定の大きさとする。

【００２６】次に、画像特徴情報抽出部１０２は、各ブロック画像の特徴を抽出し（ステップＳ１０３）、更に抽出した特徴量を符号化し、印刷できるように視覚化する（ステップＳ１０４）。このステップＳ１０４における画像の特徴抽出方法としては例えば次のようなものがある。

(1)ブロック画像を周波数変換し、周波数スペクトルをサンプリングしたもの。

(2)ブロック画像に対して、フィルタリング処理（帯域通過フィルタや任意のパターンのテンプレートなどによるフィルタリング処理）を行って得られる値。

(3)ブロック画像中の白い画素（背景領域）と、黒画素（文字領域）の面積の比。

等がある。本具体例では、周波数スペクトルをサンプリングしたものを画像の特徴情報として以下の説明を行う。

【００２７】図５は、上記ステップＳ１０２で分割されたブロック画像の一つを表す説明図である。図６は、図５のブロックに対して二次元フーリエ変換を行った結果を示す説明図である。図６は、周波数スペクトルを表しており、色が薄いほど値が大きいものとする。中心部分は直流成分とし、画像の端に近いほど高い周波数成分のスペクトルを表す。このように表される周波数特性を符号化するために、画像特徴情報抽出部１０２は、図６の特定の周波数領域のスペクトル値を数値化する。図７は、特定の周波数領域の選択の一例を示す説明図である。図中の、破線で示した円が選択した周波数領域を表し、ここでは四つの周波数領域を選択した例を示している。選択する周波数領域は、文書画像中の文字領域が持つ周波数特性をよく表し、かつ、印刷とスキャンにより生じる雑音成分により影響されないようなものを予め定めておく。又、周波数スペクトルの数値化は、対応する領域の平均スペクトル値を量子化することによって行う。図７の例では、一例として８段階（０～７）にサンプリングしている。

【００２８】図８は、ブロックの画像的特徴から視覚的なパターンを生成する処理の説明図である。即ち、図８のブロック番号情報８０１に示すように、ブロックの番号を符号化し、かつ、ブロック画像特徴情報８０２に示すように画像特徴を符号化し、パターンブロック８０３のような視覚的なパターンを生成している。ここでは、ブロック番号と画像特徴の情報を２０ビットの符号化を行う例を示している。図７では、四つの特徴量をそれぞれ８段階（３ビット）で表しているため、画像特徴は３×４＝１２ビットとなり、残りの８ビットでブロック番号を表している。尚、ここでは符号長を２０ビットとしているが、任意の長さが選択可能である。また、符号を暗号化してもよいし、任意のハッシュ関数により圧縮してもよい。図８のパターンブロック８０３は５行４列の行列であり、行列中の要素が黒ならば０を、白ならば１を表すものとする。尚、パターンブロックのこのような行列で表わすことに限らず、一般のバーコードで表現してもよい。以上で、画像特徴情報抽出部１０２によるステップＳ１０３，Ｓ１０４の処理が終了する。

11

【００２９】次に、画像特徴情報埋め込み部１０３により、文書画像中に、ステップＳ１０４で作成したパターンブロック（入力文書画像から生成される全てのブロック画像に対するパターンブロック）を文書画像中に挿入する（ステップＳ１０５）。そして、文書画像出力部１０４により、このような文書画像を印刷する（ステップＳ１０６）。図９は、印刷された文書の説明図である。図示のように、パターンブロック（元画像特徴情報部分）は入力文書画像の文字のない領域（背景領域）に挿入する。

【００３０】次に、改ざん判定装置２００の動作を説明する。図１０は、改ざん判定装置２００の動作を示すフローチャートである。改ざん判定装置２００では、先ず、印刷文書１のような判定対象文書を文書画像読み取り部２０１によって画像として読み取って、コンピュータ上のメモリに展開する（ステップＳ２０１）。また、文書画像読み取り部２０１は、読み取った画像に対して回転補正や拡大縮小や雑音除去を行い、更に、元画像特徴情報であるパターンブロック部分を切り出す。次に、埋め込み情報抽出部２０２は、文書画像読み取り部２０１で切り出されたパターンブロックにおける各ブロック画像に対する特徴量を復号する（ステップＳ２０２）。即ち、埋め込み情報抽出部２０２は、上述した画像特徴情報抽出部１０２によるパターンブロックの生成処理の逆の処理を行うことによって各ブロック画像の特徴量の復号を行うものである。

【００３１】一方、画像特徴情報抽出部２０３は、文書画像読み取り部２０１で切り出したパターンブロック部分を背景領域でマスクし、その画像に対して、上記の文書画像出力装置１００におけるステップＳ１０２およびＳ１０３の処理と同様の処理を行う（ステップＳ２０３）。次に、判定部２０４は、埋め込み情報抽出部２０２が抽出した埋め込み情報と、画像特徴情報抽出部２０３で得た各ブロック画像の画像特徴情報とをブロック毎に比較し（ステップＳ２０４）、これらの値の差が所定範囲内に収まっているかにより改ざん判定を行う（ステップＳ２０５）。

【００３２】次に、改ざんが行われた文書の例を説明する。図１１は、印刷文書に対する改ざんが行われた文書の説明図である。図１２は、改ざん箇所のブロックを示す説明図である。図１３は、改ざん箇所のブロックの画像特徴を抽出した結果の説明図である。図１１に示すように、印刷文書に対して改ざんが行われたとする。図１２は、その改ざん箇所のブロックであり、図５に対応するものである。また、図１３は、図１２のブロックの周波数スペクトルと選択された領域の説明図であり、図７に対応するものである。

【００３３】改ざん判定装置２００において、埋め込み情報抽出部２０２で復号したパターンブロックのブロック番号Ｎに対する画像特徴Ａ～Ｄの各値を、Ｐ（Ｎ，Ａ）、Ｐ（Ｎ，Ｂ）、Ｐ（Ｎ，Ｃ）、Ｐ（Ｎ，Ｄ）とし、画像特徴情報抽出部２０３で抽出したブロック番号Ｎに対する画像特徴Ａ～Ｄの各値をＱ（Ｎ，Ａ）、Ｑ（Ｎ，Ｂ）、Ｑ（Ｎ，Ｃ）、Ｑ（Ｎ，Ｄ）とする。また、同じブロック番号をもつブロック画像間の特徴量の差分Ｄ（Ｎ）を例えば、Ｄ（Ｎ）＝ＡＢＳ（Ｐ（Ｎ，Ａ），Ｑ（Ｎ，Ａ））＋ＡＢＳ（Ｐ（Ｎ，Ｂ），Ｑ（Ｎ，Ｂ））＋ＡＢＳ（Ｐ（Ｎ，Ｃ），Ｑ（Ｎ，Ｃ））＋ＡＢＳ（Ｐ（Ｎ，Ｄ），Ｑ（Ｎ，Ｄ））と定義する。ここで、ＡＢＳ（Ｘ，Ｙ）はＸとＹの差の絶対値である。

【００３４】本具体例では、図７より、Ｐ（Ｎ，Ａ）＝４、Ｐ（Ｎ，Ｂ）＝２、Ｐ（Ｎ，Ｃ）＝６、Ｐ（Ｎ，Ｄ）＝３である。また、図１３より、Ｑ（Ｎ，Ａ）＝１、Ｑ（Ｎ，Ｂ）＝７、Ｑ（Ｎ，Ｃ）＝３、Ｑ（Ｎ，Ｄ）＝２である。従って、Ｄ（Ｎ）は、｜４－１｜＋｜２－７｜＋｜６－３｜＋｜３－２｜＝１２となる。ここで、改ざん検出のための閾値Ｔを予め定めておき、Ｄ（Ｎ）がＴより大きければ、判定部２０４は、ブロック番号Ｎのブロックに対して改ざんが行われたと判定する。

【００３５】〈効果〉以上のように、具体例１によれば、文書画像の画像的特徴を文書中に印刷するので、その文書をスキャナ等で読み取って処理するだけで、改ざんの有無を判定することができる。即ち、ＯＣＲ等によりその文書の内容がどのようなものであるかを認識するといった処理は一切必要なく、文書画像の処理のみで改ざんの有無を検出することができ、大規模なシステムを必要としない効果がある。また、複数のブロックに分割するようにすれば、改ざんが行われた場合の位置の特定も可能であり、かつ、分割数を選択することによって位置特定の精度も自由に選択することができるという効果がある。

【００３６】《具体例２》具体例２は、文書画像の画像特徴情報を暗号鍵として用い、この暗号鍵を用いて隠し情報を暗号化して文書画像への埋め込み情報としたものである。

【００３７】〈構成〉図１４は、具体例２の構成図である。図のシステムは、文書画像出力装置１００ａと改ざん判定装置２００ａからなる。文書画像出力装置１００ａは、文書画像格納部１０１、画像特徴情報抽出部１０２、隠し情報格納部１１０、暗号鍵生成部１１１、隠し情報暗号化部１１２、暗号ブロック埋め込み部１１３、文書画像出力部１１４からなる。文書画像格納部１０１および画像特徴情報抽出部１０２は、具体例１と同様の機能を有するものである。隠し情報格納部１１０は、文書画像出力装置１００ａから出力される印刷文書１に暗号化されて付与される隠し情報を格納する機能部であり、磁気記憶装置や半導体メモリといった記憶装置上に実現されている。また、本具体例では隠し情報として、

その文書に対する署名情報といった情報を用いている。暗号鍵生成部１１１は、画像特徴情報抽出部１０２で抽出された画像特徴情報から暗号鍵を生成する機能部である。隠し情報暗号化部１１２は、暗号鍵生成部１１１で生成された暗号鍵を用いて隠し情報格納部１１０に格納されている隠し情報を暗号化して、文書画像中に埋め込む処理を行う機能部である。文書画像出力部１１４は、暗号ブロック埋め込み部１１３から出力された文書画像データを印刷出力するプリンタ等の機能部である。

【００３８】改ざん判定装置２００ａは、文書画像読み取り部２０１、画像特徴情報抽出部２０３、暗号鍵生成部２１０、暗号化情報抽出部２１１、隠し情報復号部２１２からなる。ここで、文書画像読み取り部２０１および画像特徴情報抽出部２０３は、具体例１と同様の構成であるため、ここでの説明は省略する。暗号鍵生成部２１０は、画像特徴情報抽出部２０３で抽出された画像特徴情報に基づいて暗号鍵を生成する機能部であり、文書画像出力装置１００ａにおける暗号鍵生成部１１１と同様の機能を有している。暗号化情報抽出部２１１は、文書画像読み取り部２０１で切り出された暗号化情報部分から暗号化情報を抽出する機能部である。隠し情報復号部２１２は、暗号鍵生成部２１０で生成した暗号鍵を用いて、暗号化情報抽出部２１１で抽出した暗号化情報を復号する機能部である。即ち、その文書に改ざんが行われていない場合は、正当な暗号鍵によって復号されるため、文書画像出力装置１００ａで付与した隠し情報が取り出せることによって、改ざんの有無を判定するものである。

【００３９】〈動作〉図１５は、文書画像出力装置１００ａの動作を示すフローチャートである。図において、ステップＳ３０１～ステップＳ３０３は、具体例１における図２のステップＳ１０１～ステップＳ１０３と同様であるため、ここでの説明は省略する。次に、暗号鍵生成部１１１は、ステップＳ３０３で抽出された各ブロックの特徴から暗号鍵を生成する。即ち、各ブロックからは部分鍵を生成し、全ての、または一部のブロックから生成される部分鍵を統合して最終的な暗号鍵とする。ここでは、その一例として、画像特徴を図７で示したように四つの周波数領域のスペクトル平均とする。また、ブロック番号Ｎに対する画像特徴Ａ～Ｄの各値をＰ（Ｎ，Ａ）、Ｐ（Ｎ，Ｂ）、Ｐ（Ｎ，Ｃ）、Ｐ（Ｎ，Ｄ）とする。このブロックから生成される部分鍵を、Ｋ（Ｎ）＝Ｈ（Ｐ（Ｎ，Ａ）、Ｐ（Ｎ，Ｂ）、Ｐ（Ｎ，Ｃ）、Ｐ（Ｎ，Ｄ））とする。ここで、Ｈ（Ａ，Ｂ，Ｃ，Ｄ）は、Ａ～Ｄの値を入力パラメータとする関数であり、ハッシュ関数などでも良い。また、最終的な暗号鍵を、ＣＫ＝Ｆ（Ｋ（１），Ｋ（２），…，Ｋ（ｎ－１），Ｋ（ｎ））（ｎはブロックの数）で表す。Ｆは部分鍵Ｋ（１）～Ｋ（ｎ）を入力パラメータとする関数である。

【００４０】次に、隠し情報暗号化部１１２は、隠し情報格納部１１０から所定の隠し情報を入力し（ステップＳ３０５）、暗号鍵生成部１１１がステップＳ３０４で生成した暗号鍵を用いて隠し情報を暗号化する（ステップＳ３０６）。尚、ここでは、暗号化と復号で同じ鍵を用いる対称暗号を用いるが、一般の共通鍵暗号でも良いし、ドットパターンの区切り位置を分からなくするようなものであっても良い。隠し情報暗号化部１１２で、隠し情報の暗号化が行われると、暗号ブロック埋め込み部１１３は、その暗号文をバーコードや具体例１で説明したパターンブロックなどによって視覚的に表現し、文書画像の空白部分に挿入する（ステップＳ３０７）。そして、文書画像出力部１１４は、これを印刷出力する（ステップＳ３０８）。ここで印刷された印刷文書１ａは、図９に示した例と視覚的には同様のものとなる。

【００４１】次に、改ざん判定装置２００ａの動作を説明する。図１６は、改ざん判定装置２００の動作を示すフローチャートである。改ざん判定装置２００ａでは、先ず、判定対象文書である印刷文書１ａを文書画像読み取り部２０１によって画像として読み取って、コンピュータ上のメモリに展開する（ステップＳ４０１）。このステップＳ４０１の処理は、具体例１のステップＳ２０１の動作と同様である。次に、暗号化情報抽出部２１１は、文書画像読み取り部２０１で切り出した暗号化情報部分から暗号文を復元する。ここでは、ステップＳ３０３でパターンブロックを生成したときと逆の処理を行うことによって、暗号文を復元することができる。

【００４２】また、画像特徴情報抽出部２０３では、暗号化情報部分を背景領域でマスクした画像に対して、先ず、画像特徴情報抽出部１０２が行うステップＳ３０２、Ｓ３０３と同様の処理を行って画像特徴情報を検出する（ステップＳ４０３）。次に、暗号鍵生成部２１０は、暗号鍵生成部１１１と同様の処理を行って、暗号鍵を生成する（ステップＳ４０４）。そして、隠し情報復号部２１２は、暗号化情報抽出部２１１で抽出した暗号文に対して暗号鍵生成部２１０で生成した暗号鍵を用いて暗号文を復号する（ステップＳ４０６）。このとき、印刷文書１ａに対して改ざんなどの不正が行われた場合は、ステップＳ４０３で抽出した画像特徴情報と、図１５のステップＳ３０３で抽出した画像特徴情報に差が生じ、これにより、ステップＳ４０４において、正しい暗号鍵が生成されないことになる。その結果、ステップＳ４０５において暗号文が正しく復号できないことになる。従って、隠し情報が意味のない（内容を理解できない）ものとなってしまう。即ち、復号された隠し情報が意味のあるものであるかどうかによって、印刷文書１ａに対して改ざんが行われたか否かをチェックする。

【００４３】〈効果〉以上のように、具体例２によれば、署名情報等の隠し情報を印刷文書の画像的特徴による暗号鍵を用いて暗号化し文書に埋め込むようにしたため、印刷文書に対して改ざんなどの不正が行われない場

15

合にのみ埋め込んだ情報を確認することができる。従って、署名の確認と印刷内容の確認を同時に行うことができる。

【００４４】尚、上記各具体例では、元画像特徴情報や暗号化情報を文書上に視覚的に印刷するようにしたが、これ以外にも、例えば印刷文書１（１ａ）上に磁気ストライプ部を設け、この磁気ストライプに磁気データとして記録するといった構成であってもよい。また、このような場合は、改ざん判定装置２００（２００ａ）側でも磁気データの読み取り手段を設けることが必要である。

【図面の簡単な説明】

【図１】本発明の改ざん判定システムの具体例１を示す構成図である。

【図２】具体例１の文書画像出力装置の動作を示すフローチャートである。

【図３】文書画像の一例を示す説明図である。

【図４】文書画像を分割した状態の説明図である。

【図５】分割されたブロック画像の一つを表す説明図である。

【図６】図５のブロックに対して二次元フーリエ変換を行った結果を示す説明図である。

【図７】特定の周波数領域の選択の一例を示す説明図である。

【図８】ブロックの画像的特徴から視覚的なパターンを生成する処理の説明図である。

【図９】印刷された文書の説明図である。

16

【図１０】具体例１の改ざん判定装置の動作を示すフローチャートである。

【図１１】印刷文書に対する改ざんが行われた文書の説明図である。

【図１２】改ざん箇所のブロックを示す説明図である。

【図１３】改ざん箇所のブロックの画像特徴を抽出した結果の説明図である。

【図１４】具体例２の構成図である。

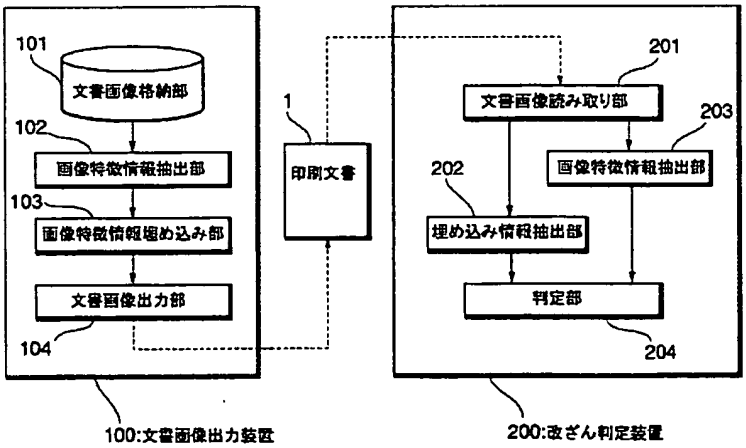
【図１５】具体例２の文書画像出力装置の動作を示すフローチャートである。

【図１６】具体例２の改ざん判定装置の動作を示すフローチャートである。

【符号の説明】

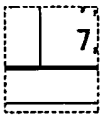
１、１ａ　印刷文書
１００、１００ａ　文書画像出力装置
１０２、２０３　画像特徴情報抽出部
１０３　画像特徴情報埋め込み部
１０４、１１４　文書画像出力部
１１１、２１０　暗号鍵生成部
１１２　隠し情報暗号化部
１１３　暗号ブロック埋め込み部
２００、２００ａ　改ざん判定装置
２０２　埋め込み情報抽出部
２０４　判定部
２１１　暗号化情報抽出部
２１２　隠し情報復号部

【図１】



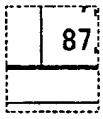
具体例１の構成図

【図５】



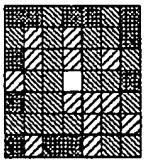
ブロック画像の説明図

【図１２】



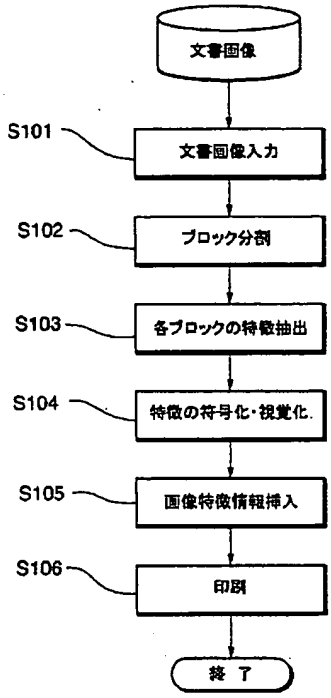
改ざん箇所のブロックの説明図

【図６】



二次元フーリエ変換を行った結果の説明図

【図２】



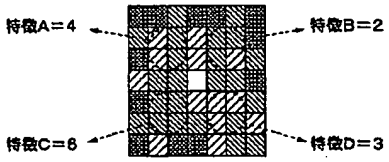
具体例1の文書画像出力装置の動作フローチャート

【図３】

日付	摘要	収入	支出	差引残高
11月分				
11.5	コート代(10.18)		870	28,814
11.5	コート代(10.25)		870	27,944
11.5	ボール代(10.25)		1,852	26,092
11.10	コート代(11.9)		1,110	24,982
11.21	コート代(10.3)		7,000	17,982
11.21	コート代(10.17)		7,000	10,982
下期				
	部費	¥30,000	コート代	¥50,670
	全友会	¥15,000	ボール代	¥5,506
	参加費	¥18,000		
	寄付	¥9,000		
計		¥72,000		¥56,176

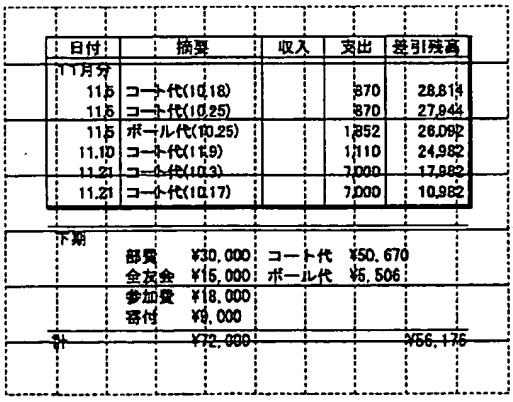
文書画像の説明図

【図７】



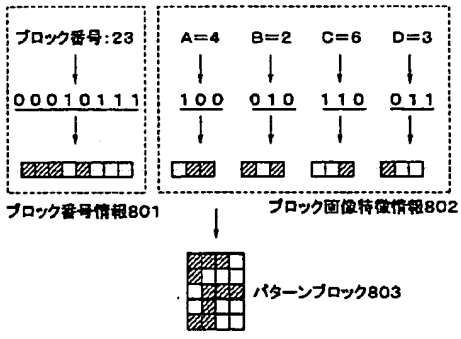
特定の周波数領域の選択の一例の説明図

【図４】



文書画像を分割した状態の説明図

【図８】



ブロックの画像的特徴から視覚的なパターンを生成する処理の説明図

【図９】

日付	摘要	収入	支出	差引残高
11月分				
11.5	コート代(10.18)		870	28,814
11.5	コート代(10.25)		870	27,944
11.5	ボール代(10.25)		1,852	26,092
11.10	コート代(11.9)		1,110	24,982
11.21	コート代(10.3)		7,000	17,982
11.21	コート代(10.17)		7,000	10,982

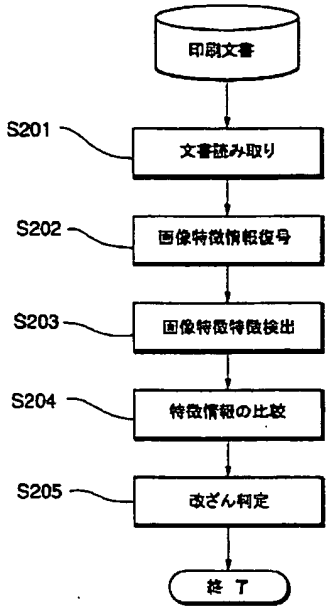
下期

部費	¥30,000	コート代	¥50,670
全友会	¥15,000	ボール代	¥5,506
参加費	¥18,000		
寄付	¥9,000		
計	¥72,000		¥56,176

画像特徴情報（パターンブロック）

印刷文書の説明図

【図１０】



具体例1の改ざん判定装置の動作フローチャート

【図１１】

日付	摘要	収入	支出	差引残高
11月分				
11.5	コート代(10.18)		870	28,814
11.5	コート代(10.25)		870	27,944
11.5	ボール代(10.25)		1,852	26,092
11.10	コート代(11.9)		1,110	24,982
11.21	コート代(10.3)		7,000	17,982
11.21	コート代(10.17)		87,000	10,982

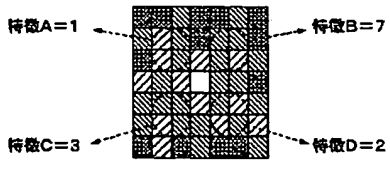
改ざん箇所

下期

部費	¥30,000	コート代	¥50,670
全友会	¥15,000	ボール代	¥5,506
参加費	¥18,000		
寄付	¥9,000		
計	¥72,000		¥56,176

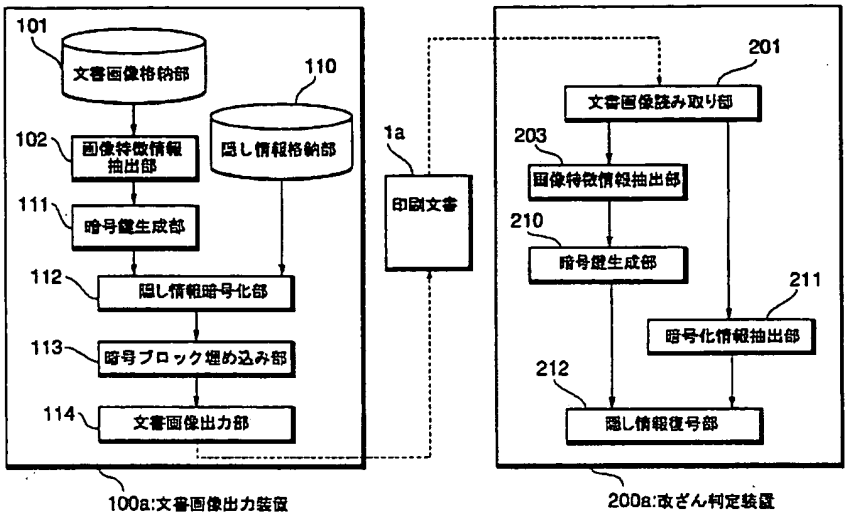
改ざんが行われた文書の説明図

【図１３】



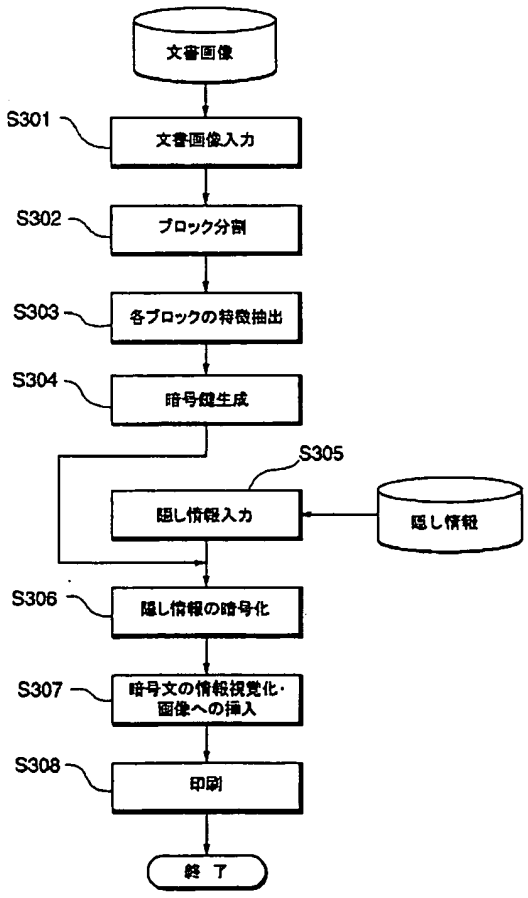
改ざん箇所のブロックの画像特徴抽出結果の説明図

【図１４】



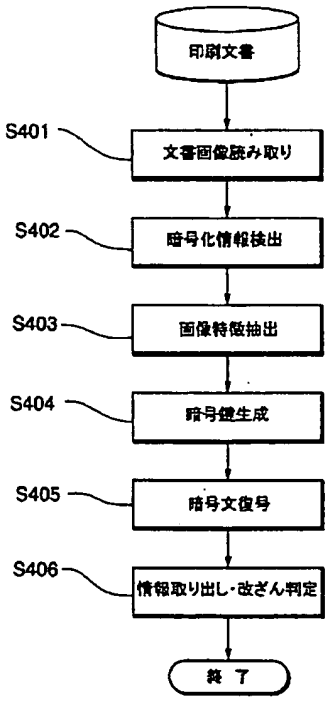
具体例２の構成図

【図１５】



具体例2の文書画像出力装置の動作フローチャート

【図１６】



具体例2の改ざん判定装置の動作フローチャート

フロントページの続き

(51)Int.Cl.'	識別記号	Ｆ Ｉ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０９Ｃ　5/00		Ｇ０９Ｃ　5/00	

Ｆターム(参考)　2C061 HK11 HN15
2C187 BF26 DB21 GD01
5B057 AA11 AA20 BA02 CB19 CE08
CE09 CE20 CG07 DC01 DC36
5C076 AA14 BA06
5J104 AA08 NA02